

FY09 Tactical Plan for **Computing Infrastructure (CI)**

Prepared by: Matt Arena

Date: 15 June 2008

Relevant Strategic Plan — [Strategic Plan for Central Services FY2007-FY2009](#)

CI Goal —

- Facilitate efficient user utilization of Lab computing resources
- Support and develop Lab information technology infrastructure.

CI Strategy —

- Support and develop computational infrastructure applications as part of Central Services' mission.
- Implement ITIL practices into our project lifecycle.

Objectives for FY09

1. Continue development and support of Network Infrastructure and Management Infrastructure (NIMI) and dependant applications.
 - a. NIMI database.
 - b. Tissue database.
 - c. Network Inventory database
 - d. Nimrod
2. Provide support for CD's ability to monitor its IT infrastructure re-designing NGOP or selecting a vendor solution.
3. Provide support for the Central Services.
 - a. Grid services.
 - b. Computer resource accounting and capacity planning
 - c. Networking
 - d. Computer Security
4. Have project leaders complete ITIL training.

Computing Infrastructure / Monitoring Tools.

- Activity Type: New
- Timescale: FY09 Q4
- Milestones: Completion of a design, implementation and rollout.
- Metrics: Acceptance of a design to efficiently monitor all network elements, scalability and ease of maintenance.

Computing Infrastructure / Grid Services

- Activity Type: Ongoing
- Timescale: FY09
- Milestones:
- Metrics:

Computing Infrastructure /Resource Accounting

- Activity Type: Project
- Timescale: FY09
- Milestones:
- Metrics:

Computing Infrastructure / Networking and Computer Security

- Activity Type: Ongoing
- Timescale: FY09
- Milestones:
- Metrics:

Priorities

1. Develop and support applications for the Computer Security Team to meet regulatory requirements.
2. ITIL training for all project leaders.
3. Support Networking
4. Support Grid Services
5. Develop and support applications for NIMI, TIssue, Network Inventory, Nimrod
6. Design and support of Computing Resource Accounting database application.
7. Upgrade or replace existing monitoring system (NGOP).
8. Bring applications built using old technologies to the new technology base.

Staffing: No change to current (or planned) staffing is required.

Risk Assessment:

1. Failure to meet regulatory compliance in the Computer Security realm may result in additional restrictions imposed upon Fermilab.
2. Failure to properly train personnel in ITIL will result in a delay of ISO 20000 certification.
3. Failure to support Networking may result in unsatisfactory service provided to the Fermilab community.
4. Failure to support Grid Services may result in unsatisfactory service provided to the Fermilab community.
5. Failure to support NIMI will result in decrease productivity in Networking and CST, a likely increase in problematic machines due to vulnerabilities and an increase in FCIRT issues.
6. Failure to design and support a new Computing Resource Accounting database application will result in
7. Failure to upgrade or replace NGOP will result in less systems being monitored.
8. We also recognize the fact that support of applications built on old technologies requires increasing level of support, which is not always easy to even predict. We need to proactively invest some effort in the modernization of our old applications even if they appear to be in good shape now.